

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-215826

(43)Date of publication of application : 02.08.2002

(51)Int.Cl.

G06F 17/60

G09C 1/00

H04L 9/32

(21)Application number : 2001-011961

(71)Applicant : HITACHI LTD

(22)Date of filing : 19.01.2001

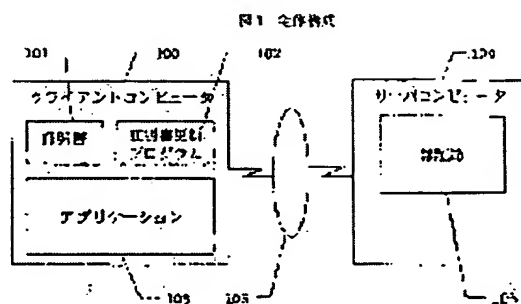
(72)Inventor : IBA KENICHI
IKEUCHI MANABU
BANDAI KENSUKE

(54) DEVICE AND METHOD FOR AUTOMATIC CERTIFICATE RENEWAL

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a device for automatic certificate renewal which can automatically renew a certificate when the certificate, which has necessary information for renewal itself, will be expired soon or has already expired.

SOLUTION: A certificate renewal program 102, which is connected to a server computer 104 with a certificate authority function and automatically renews the certificate, a storage which stores the certificate, and an application program 103 which uses the certificate are prepared. A client computer 100 is connected to the server computer and requests the server computer to renew the certificate automatically after or at the last days of the expiring date of the certificate. The certificate has a certificate renewal program execution part which executes expiring information and the certificate renewal program. The certificate is connected to the server computer 104 and requests the server computer to renew the certificate automatically after or at the last days of the expiring date of the certificate, besides it receives a renewed certificate and stores it in the storage.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-215826

(P2002-215826A)

(43) 公開日 平成14年8月2日 (2002.8.2)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テ-マ-ト ⁷ (参考) |
|---------------------------|-------|---------------|-------------------------|
| G 0 6 F 17/60 | 1 4 0 | G 0 6 F 17/60 | 1 4 0 5 J 1 0 4 |
| G 0 9 C 1/00 | 6 4 0 | G 0 9 C 1/00 | 6 4 0 Z |
| H 0 4 L 9/32 | | H 0 4 L 9/00 | 6 7 5 D |

審査請求 未請求 請求項の数 5 O L (全 7 頁)

(21) 出願番号 特願2001-11961 (P2001-11961)

(22) 出願日 平成13年1月19日 (2001.1.19)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 伊庭 健一

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

(72) 発明者 池内 学

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

(74) 代理人 100093492

弁理士 鈴木 市郎 (外1名)

最終頁に続く

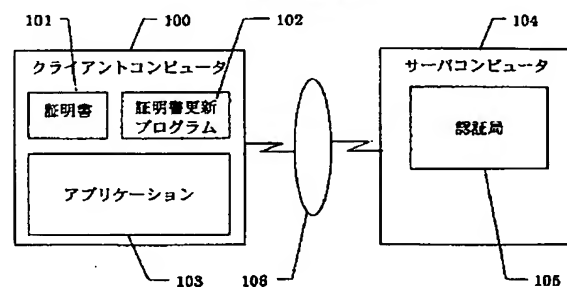
(54) 【発明の名称】 証明書自動更新装置および方法

(57) 【要約】

【課題】 証明書の更新作業に必要な情報を証明書自身に持たせて有効期限間近になった場合、あるいは失効した場合に、自動的に証明書を更新することのできる証明書自動更新装置を提供する。

【解決手段】 認証局機能を有するサーバコンピュータ104に接続して証明書を自動更新する証明書更新プログラム102および前記証明書を格納する記憶装置と、前記証明書を利用するアプリケーションプログラム103とを備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータ100からなり、前記証明書は有効期限情報および前記証明書更新プログラムを起動する証明書更新プログラム起動部を備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータ104に接続して前記サーバコンピュータに前記証明書の自動更新を要求するとともに、更新された証明書を受信して前記記憶装置に格納する。

図1 全体構成



【特許請求の範囲】

【請求項 1】 認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、前記証明書を利用するアプリケーションプログラムとを備え、

前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータからなり、

前記証明書は有効期限情報および前記証明書更新プログラムを起動する証明書更新プログラム起動部を備えたことを特徴とする証明書自動更新装置。

【請求項 2】 請求項 1 の記載において、前記クライアントコンピュータはリムーバブル媒体に前記証明書情報を格納するリムーバブル媒体駆動装置を備えたことを特徴とする証明書自動更新装置。

【請求項 3】 認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、

前記証明書を利用するアプリケーションプログラムとを備え、

前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータからなる証明書自動更新方法であって、前記証明書自動更新方法は、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するステップと、前記証明書更新プログラムを起動するステップと、サーバコンピュータに接続するステップと、サーバコンピュータから証明書の発行を受けるステップと、受けた証明書を記憶装置に蓄積するステップとを含むことを特徴とする証明書自動更新方法。

【請求項 4】 クライアントコンピュータに格納した証明書の有効期限の末期あるいは有効期限の終了後に、認証機能を有するサーバコンピュータに接続して該サーバコンピュータに前記証明書の自動更新を要求するステップと、該要求に基づきクライアントコンピュータに格納した証明書更新プログラムを起動するステップと、クライアントコンピュータをサーバコンピュータに接続するステップと、サーバコンピュータから証明書の発行を受けるステップと、受けた証明書を記憶装置に蓄積するステップとを含むプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 5】 認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、前記証明書を利用するアプリケーションプログラムと認証局機能を有し、少なくとも認証局のアドレス情報を含

む証明書を発行するサーバとを備え、

前記クライアントコンピュータは前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するとともに、更新された証明書を受信して前記記憶装置に格納することを特徴とする証明書自動更新システム。

【発明の詳細な説明】

【0001】

10 【発明の属する技術分野】本発明は認証局によって発行される公開鍵証明書を自動的に更新することのできる証明書自動更新装置および更新方法に関する。

【0002】

【従来の技術】近年、インターネット技術が急速に普及し、これに伴い、インターネットあるいはイントラネット上でのデータの盗聴、改ざん、成りすまし等のセキュリティ上の問題が発生してきた。このような問題を解決するため、現在では公開鍵暗号方式を使用したセキュリティ技術が一般的に採用されるようになった。公開鍵暗号方式は、秘密鍵および公開鍵からなる一対の鍵を使用し、前記秘密鍵は他人に漏れないように秘密裡に保管する。一方、公開鍵は他人に公開し、自己に対する暗号文作成等に使用される。このため前記公開鍵とその所有者の関係は第 3 者によって保証されなければならない。この保証は、通常は前記第 3 者機関である認証局が公開鍵証明書を発行することにより行われる。

【0003】

【発明が解決しようとする課題】前記従来技術においては、前記証明書を使用するユーザーは、認証局から発行された証明書の有効期限が間近になった場合、あるいは失効してしまった場合においては、Web ブラウザを介して認証局のホームページにアクセスして、その認証局における証明書の更新手順に従って証明書の更新登録作業を行わなければならない。すなわち、前記証明書の更新作業は、人手を介して行うことから、証明書の更新忘れ、更新手順忘れ等が頻繁に生じていた。

【0004】ユーザー認証、暗号化、復号化、署名、検定等を行うアプリケーションの中には、証明書の有効期限が間近の場合には、その旨のメッセージを表示してユーザーにその後の証明書の更新作業を促し、さらに、期限切れの場合はエラーメッセージを表示してアプリケーションを停止したり、あるいは証明書を必要とする機能を制限してアプリケーションを立ち上げるものがある。この場合において、証明書を更新するには、一旦アプリケーションを停止して再起動することが必要である。

【0005】本発明は前記問題点に鑑みてなされたもので、証明書の更新作業に必要な情報を証明書自身に持たせて有効期限間近になった場合、あるいは失効した場合に、自動的に証明書を更新することのできる証明書自動更新装置を提供することにある。

【0006】

【課題を解決するための手段】本発明は、上記の課題を解決するために次のような手段を採用した。

【0007】認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、前記証明書を利用するアプリケーションプログラムとを備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータからなり、前記証明書は有効期限情報および前記証明書更新プログラムを起動する証明書更新プログラム起動部を備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するとともに、更新された証明書を受信して前記記憶装置に格納する。

【0008】

【発明の実施の形態】以下に本発明の実施形態を図1ないし図5を用いて説明する。図1は、本発明を説明するための全体構成図である。図において、100は証明書を使用するユーザーの保有するクライアントコンピュータである。101はクライアントコンピュータ100のハードディスク等の記憶装置に格納された証明書である。102は認証局に接続し証明書を実際に更新するための証明書更新プログラムである。103は証明書101を使用して暗号化、署名付与等のセキュリティ技術を使用するアプリケーションである。このアプリケーションは、証明書101を使用するアプリケーションであれば、Webブラウザでもユーザーが独自に開発した業務用アプリケーションでもいかなるアプリケーションであってもよい。104は証明書101を発行する認証局機能を備えたサーバコンピュータである。105はサーバコンピュータ104上に構築した認証局である。106はクライアントコンピュータ100とサーバコンピュータ104を接続している広域ネットワークである。

【0009】図2は、証明書101の格納先がICカードである場合のクライアントの構成例である。200はICカード内の情報を読み書きするためのクライアントコンピュータ100に接続したICカードリーダー・ライターである。201は証明書101を格納したICカードである。本発明によれば、ハードディスクに格納された証明書101だけでなく、ICカード201に格納した証明書101の自動更新も行うことができる。

【0010】図3は、証明書101の格納先がリムーバブル媒体である場合のクライアントの構成例である。300はリムーバブル媒体内の情報を読み書きするためのクライアントコンピュータ100に接続されているリムーバブル媒体駆動装置である。301は証明書101を格納したリムーバブル媒体である。リムーバブル媒体3

01としては、例えばフロッピー（登録商標）ディスク、光磁気ディスクなどがあげられる。本発明によれば、ハードディスクに格納した証明書101だけでなく、リムーバブル媒体301に格納した証明書101の自動更新も行うことができる。

【0011】図4は、前記認証局により証明書101に記録する情報の一例である。400は証明書101の有効期限開始日である。401は証明書101の有効期限終了日である。402は認証局アドレス情報である。この認証局アドレス情報402は、認証局105への接続仕様に依存し、URLあるいはIPアドレスとすることができる。403は認証局アドレス情報402を参照して認証局105に接続し、証明書101を更新するための証明書更新プログラム名称であり、例えば証明書更新プログラム102を指定する。404は前記証明書更新プログラム102を実際に起動するための証明書更新プログラム起動部である。証明書101に対してアプリケーション103からアクセスが行われた場合には、この証明書更新プログラム起動部がまず動作する。405は前記証明書更新プログラム102を起動する手順を示した証明書更新プログラム起動手順である。406は証明書の自動更新を有効期限終了日401の何日前から行うようにするかを指定した自動更新開始パラメタである。

【0012】図5は、証明書自動更新装置における全体的なシーケンスの一例を示したものである。ユーザー500はアプリケーション103を起動501する。アプリケーション103は起動すると、暗号化および署名などを行うのに必要となる証明書101にアクセス502する。証明書101の格納先は、クライアントコンピュータ100内のハードディスク、ICカード201あるいはフロッピーディスク等のリムーバブル媒体301のいずれかである。

【0013】前記証明書101の有効期限終了日401が現在時刻の間近となっているかまたは失効している場合は、証明書に格納された証明書更新プログラム起動手順405に従い証明書更新プログラム名称403で示す証明書更新プログラム102を起動503する。一方、証明書101の有効期限終了日401が現在時刻の間近になっていなく、かつ失効していない場合はそのままアプリケーション103に制御を復帰504する。

【0014】証明書更新プログラム102が起動されたら、証明書101の認証局アドレス情報402に従い認証局105にネットワークを介して接続505する。続いて証明書更新プログラム102は、認証局105に対して証明書更新要求506を行う。認証局105は証明書更新依頼506を受け付けると、実際に証明書の更新に必要な情報を得るために、更新手続要求507を証明書更新プログラム102に対して発行する。更新手続要求507を受け取った証明書更新プログラム102は、ユーザー500に対してユーザーから証明書の更新に必

要な情報を得るために、更新手続要求508を発行する。

【0015】更新手続要求508を受け取ったユーザー500は、証明書の更新に必要な情報を入力509する。証明書更新プログラム102は前記入力509された情報を元に更新手続応答510を認証局105に返す。更新手続応答510を受け取った認証局105は、更新手続応答510に従い、証明書更新プログラム102に対して証明書発行511を行う。更新後の証明書を受け取った証明書更新プログラム102は、ハードディスク、あるいはICカード201、フロッピーディスク等のリムーバブル媒体301のいずれかに対して証明書格納512を行う。その後、証明書更新プログラム102は、ユーザー500に対して証明書の更新手続きが成功したことを示す証明書更新完了513を通知し、アプリケーション103に制御を復帰514する。これにより、ユーザー300は認証局105への接続を意識しなくても、自動的に接続して証明書を更新するので、ユーザは証明書101の有効期限終了日401に注意を払うことなく業務などを行うアプリケーション103を続行することができる。

【0016】図6は、証明書自動更新処理の流れ図を示したものである。既にアプリケーション103は起動されていると仮定している。まず、ステップ600において、アプリケーション103から証明書へのアクセスが行われる。ステップ601において、証明書101に格納されている証明書更新プログラム起動部404が起動される。ステップ602において、証明書更新プログラム起動部204は、自動更新開始パラメタ読み込み、ステップ603において、現在時刻の取得を行う。

【0017】ステップ604において、取得した現在時刻と証明書101に格納された有効期限終了日401を比較し、証明書の有効期限が失効している場合はステップ606に進み、失効していない場合はステップ605に進む。ステップ605において、有効期限終了日401から自動更新開始パラメタ406で指定されている日数分を減算して自動更新開始日付を求め、該日付と現在時刻と比較する。自動更新開始日付に到達している場合はステップ606に進み、そうでない場合は処理を終了する。ステップ606において、証明書更新プログラム名称、起動手順、および認証局アドレスの読み込みを行う。ステップ607において、証明書更新プログラム起動部204は前記読み込んだ情報を元に証明書更新プログラムの起動を行う。起動された証明書更新プログラム102は、ネットワークを介して認証局105と接続し、例えば図5のシーケンスで示したシーケンスを経て証明書更新手続を行う。ステップ609において、認証局105から更新後の証明書が発行されたら、該更新後の証明書を受け取って記録媒体に格納して処理を終了する。なお、格納先は更新前の証明書が格納されていた

記録媒体とすることができる。

【0018】図7は、証明書の自動更新を行った後に、更新前の古い証明書を削除するときの流れ図を示したものである。ここでは既に証明書101は有効期限間近もしくは失効していて、自動更新が行われる条件とする。まず、ステップ700において、図5、図6で詳述した証明書自動更新を行い、ステップ701において、更新後の証明書を認証局105から受け取り、受け取った証明書を格納する。ステップ702において、ダイアログメッセージを表示して、ユーザに更新前証明書を削除するかどうか問い合わせる。ユーザが削除する旨の回答を入力したときはステップ703に進み、そうでないときは処理を終了する。ステップ703において、更新前の証明書を削除する。これにより、古い証明書による記憶媒体のメモリ消費をなくすることができる。

【0019】図8は、認証局が複数存在し、その各々の認証局から証明書が発行されている場合の全体構成図を示すものである。800はサーバコンピュータAである。801はサーバコンピュータA800上に構築した認証局Aである。802はサーバコンピュータBである。803はサーバコンピュータB802上に構築した認証局Bである。804はクライアントコンピュータ100のハードディスクに格納された認証局A801から発行された証明書である。805は同様に認証局B803から発行された証明書である。認証局が複数ある場合においても、前述した単数の場合と同様の手順でそれぞれの認証局から更新後の証明書を受け取ることができる。

【0020】図9は、図8で示された構成における証明書自動更新処理の流れ図を示すものである。ここでは既に証明書A804および証明書B805は有効期限間近もしくは失効していて、自動更新が行われる条件とする。まず、ステップ900において、アプリケーション103から証明書Aへのアクセスが行われる。ステップ901において、証明書更新プログラム起動部404は、証明書更新プログラム名称、起動手順、認証局Aのアドレスの読み込みを行う。ステップ902において、読み込んだ情報を元に証明書更新プログラムを起動する。ステップ903において、起動した証明書更新プログラム102は認証局Aとの証明書更新手続を行う。ステップ904において、認証局A801から更新後の証明書が発行されると、更新後の証明書を受け取り、格納する。

【0021】ステップ905において、アプリケーション103から証明書Bへのアクセスが行われる。ステップ906において、証明書更新プログラム起動部404は、証明書更新プログラム名称、起動手順、認証局Bのアドレスの読み込みを行う。ステップ907において、読み込んだ情報を元に証明書更新プログラムを起動する。ステップ908において、起動した証明書更新プロ

グラム102は認証局Bとの証明書更新手続きを行う。ステップ909において、認証局B801から更新後の証明書が発行されると、更新後の証明書を受け取り、格納する。

【0022】以上により、複数の認証局A801及び認証局B803から発行された複数の証明書A804及び証明書B805の自動更新が終了する。これにより、認証局が複数でまた、その各々の認証局から発行された証明書を使用する構成においても、証明書の自動更新が可能となる。

【0023】以上説明したように、証明書の更新作業に必要な情報を証明書自身に持たせて有効期限間近になった場合、あるいは失効した場合に、自動的に認証局に接続して証明書を更新する。したがって、前記証明書を使用してセキュリティを確保するアプリケーションを用いて業務を行うユーザーは、証明書の有効期限や証明書発行機関である認証局への接続を意識しなくても、証明書の有効期限間近や失効した場合において、アプリケーションが証明書にアクセスしたとき、自動的に認証局へ接続し、証明書の更新を行い、そのままアプリケーションに制御を戻すことができる。このため、ユーザーはアプリケーションの停止や再起動などの煩わしさや、証明書を発行してもらうための認証局のアドレスやURLなどを調べる手間が軽減され、証明書の更新忘れによる業務の停止などを防ぐことができる。さらに、証明書を使用することのできるいかなるアプリケーションに対しても、特に手を加えることなく、前述の自動更新を実装することができる。このためユーザーに対して証明書更新の徹底を図ることが容易になる。

【0024】

【発明の効果】以上説明したように本発明によれば、証明書の更新作業に必要な情報を証明書自身に持たせて有*

* 効期限間近になった場合、あるいは失効した場合に、自動的に証明書を更新することのできる証明書自動更新装置を提供することができる。

【図面の簡単な説明】

【図1】本発明を説明するための全体構成図である。

【図2】クライアントの構成例を示す図である。

【図3】クライアントの構成例を示す図である。

【図4】証明書に記録する情報の一例を示す図である。

【図5】証明書自動更新処理における全体的なシーケンスの一例を示す図である。

【図6】証明書自動更新処理の流れ図である。

【図7】更新前の証明書を削除するときの流れ図である。

【図8】認証局が複数ある場合の全体構成図である。

【図9】証明書自動更新処理における証明書自動更新処理の流れ図である。

【符号の説明】

100 クライアントコンピュータ

101 証明書

20 102 証明書更新プログラム

103 アプリケーション

104、800、802 サーバコンピュータ

105 認証局

200 ICカードリーダー・ライター

201 ICカード

300 リムーバブル媒体駆動装置

301 リムーバブル媒体

801 認証局A

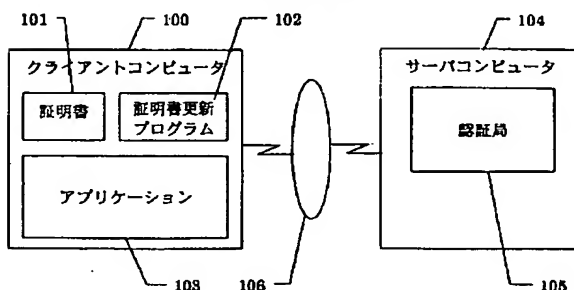
803 認証局B

30 804 証明書A

805 証明書B

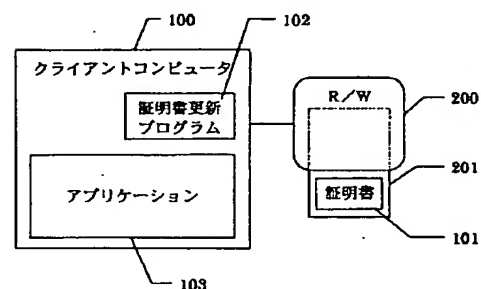
【図1】

図1 全体構成

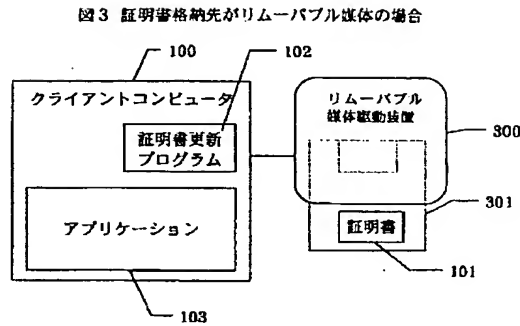


【図2】

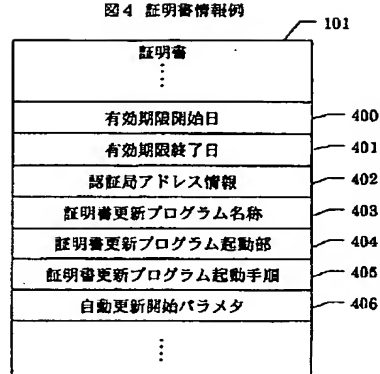
図2 証明書格納先がICカードの場合



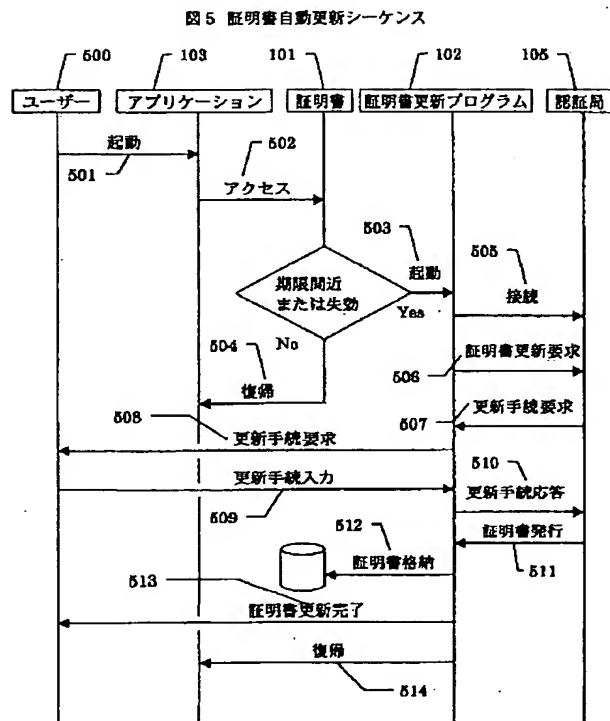
【図3】



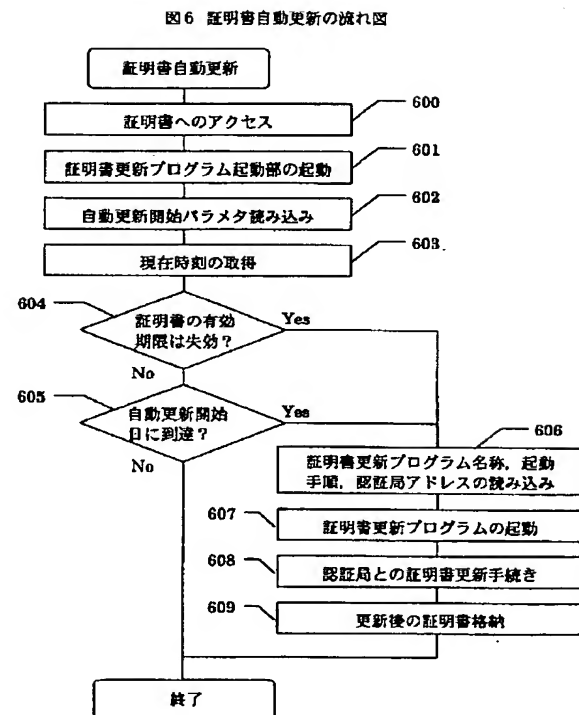
【図4】



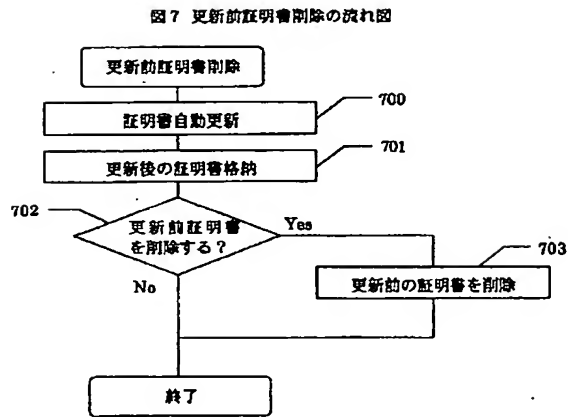
【図5】



【図6】

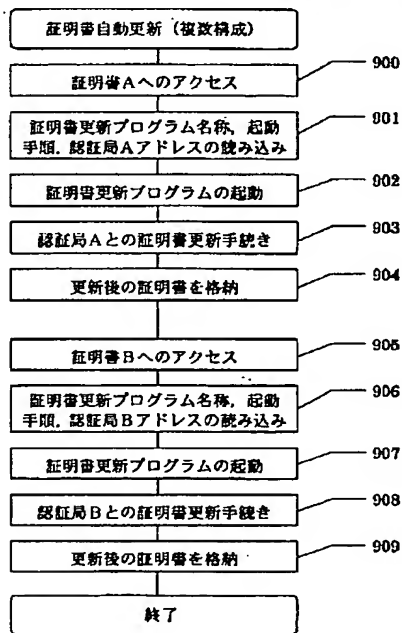


【図7】



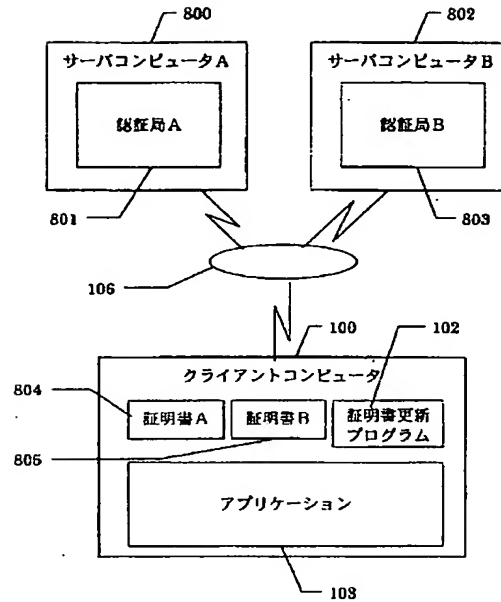
【図9】

図9 認証局と証明書が複数の場合の証明書自動更新の流れ図



【図8】

図8 認証局と証明書が複数の構成の場合



フロントページの続き

(72)発明者 萬代 健介
 神奈川県横浜市戸塚区戸塚町5030番地 株
 式会社日立製作所ソフトウェア事業部内

Fターム(参考) 5J104 AA12 MA03 NA31 NA32 NA35
 PA07

This Page Blank (uspto)